Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 37 (2014) 357 – 362

Procedia Computer Science

The 6th International Symposium on Applications of Ad hoc and Sensor Networks (AASNET'14)

State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions

Farrukh Shahzad[a]

[a]*King Fahd University of Petroleum and Minerals, Dhahran, KSA.*

Abstract

The evolution of cloud computing has revolutionized how the computing is abstracted and utilized on remote third party infrastructure. It is now feasible to try out novel ideas over the cloud with no or very low initial cost. Cloud computing is attractive to companies and organizations as it eliminates the requirement for them to plan ahead for provisioning, and allows them to start with small resources and increase gradually as the service demand rises. There are challenges in adopting cloud computing; but with obstacles, we have opportunities for research in several aspects of cloud computing. One of the main issue is the data security and privacy of information stored and processed at the cloud service provider's systems. In this work, We surveyed several research work on cloud computing related to security challenges and privacy issues. The primary goal of this paper is to provide a better understanding of the security challenges of cloud computing and identify approaches and solutions which have been proposed and adopted by the cloud service industry.

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.

Keywords: Cloud Computing; Storage Security; Cloud Storage; Data Privacy; Cloud Security

1. Introduction

Cloud computing has evolved as a popular and universal paradigm for service oriented computing where computing infrastructure and solutions are delivered as a service [1]. The cloud has revolutionized the way computing infrastructure is abstracted and used. Some of the features which makes cloud computing desirable includes; elasticity (the ability to scale on-demand), pay-per-use (which means no/low upfront investment and low time to market) and transfer of risk (from the small application developers to the large service providers) . Therefore novel applications/ideas can be tried with minimal risks, an approach that was not feasible in the pre-cloud era. This has resulted in large numbers of applications—of various types, sizes, and requirements—being deployed across the various cloud service providers. Cloud computing not only realizes the dream of computing as a utility but provides opportunity for its adoption and

* Corresponding author. Tel.: +966-556362194.
E-mail address: farrukhshahzad@kfupm.edu.sa

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.
doi:10.1016/j.procs.2014.08.053

growth. As with any new technology, there are challenges and obstacles. Data confidentiality and security are among the main obstacles in adopting the cloud service at the enterprise level[2,3].

Cloud computing is often compared to many similar technologies namely: Grid computing, Utility computing and Autonomic computing[4]. In reality, cloud leverages several aspects of these technologies but differs in many aspects. In a nut shell, cloud computing adopts virtualization technology to achieve the goal of providing computing resources as a utility.

There are many definition of cloud computing, but the definition provided by The National Institute of Standards and Technology (NIST) seems to cover all essential aspects of cloud computing[5,6].

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, and provides the opportunities for cost reduction through optimized and efficient computing. The cloud model envisages a world where components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down to provide an on-demand utility-like model of allocation and consumption[7].

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in Figure 1.

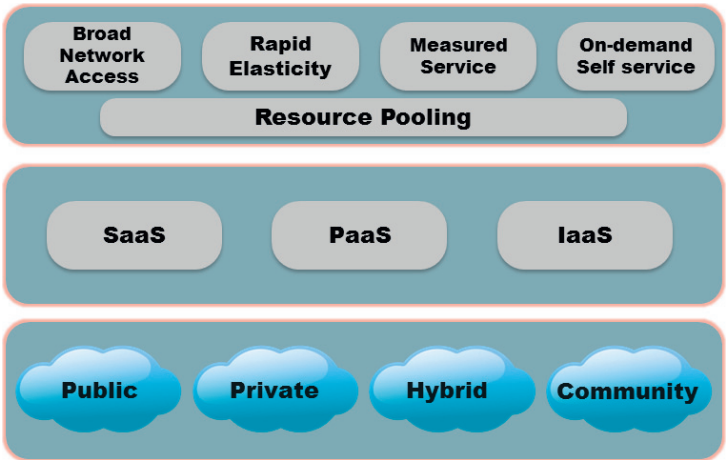

Fig. 1. Cloud computing model

1.1. Cloud Computing Characteristics

Cloud services exhibit five essential characteristics that demonstrate their similarities and differences from traditional computing approaches[7,5].

- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or data-center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned in some cases automatically to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- **Measured service**: Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the service.
- **On-demand self-service**: A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically without requiring human interaction with a service provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.

2. Security in the Cloud

Despite the tremendous business and technical advantages of the cloud, the security and privacy concern has been one of the major hurdles preventing its widespread adoption. Especially for outsourced data services, the owners exclusive control over their data is ultimately relinquished to the CSPs[8]. For example, Googles recent privacy policy implies that they essentially own the right to arbitrarily handle the uploaded user data[9]. As a result, from the data owners point of view, whenever their outsourced data contain sensitive personal information, such as financial and medical records, and social network profiles, it can no longer be considered as private as before. On the other hand, although in reality CSPs usually enforce data security through mechanisms like firewalls and virtualization, these measures do not fully guard against threats of unauthorized data access from insiders, outsiders, or other cloud tenants due to the non-bug-free deployment and low degree of transparency. Infamous data breach incidents occur from time to time, such as the recent Sony PlayStation data breach[10] and DropBox privacy leakage[11].

2.1. Risk Unique to cloud environment

The unique cloud environment raises various security and privacy concerns[12].

- **Outsourcing**: Users may lose control of their data. Appropriate mechanisms needed to prevent cloud providers from using customers data in a way that has not been agreed upon in the past.
- **Extensibility and Shared Responsibility**: There is a trade-off between extensibility and security responsibility for customers in different delivery models.
- **Virtualization**: There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host.
- **Multi-tenancy**: Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.
- **Service Level Agreement**: The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time.
- **Heterogeneity**: Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges.

2.2. eDDoS (economic Distributed Denial of Service)

Distributed Denial of Service (DDoS) attacks target web sites, hosted applications or network infrastructures by absorbing all available bandwidth and disrupting access for legitimate customers and partners. DDoS attacks can bring mission critical systems and business operations to a halt, resulting in lost revenue opportunities, decreased productivity or damage to company's reputation.

The eDDoS (economic Distributed Denial of Service) in cloud is due to the DDoS attack, where the service to the legitimate user is never restricted. But the service provider who is using cloud will incur a debilitating bill by using highly elastic (auto-Scaling) capacity to unwittingly serve a large amount of undesired traffic in order to maintain the

QoS as per the SLA. This leads to Economic Denial of Sustainability (EDoS). Hence it is necessary to drop the DDoS before the billing mechanism starts for the service provider[13].

2.3. Cloud Storage security

One of the most commonly used cloud service is data storage, where end users can outsource any amount of data to cloud servers to enjoy virtually unlimited hardware/software resources and ubiquitous access, with no or little investment. Indeed, many well-known cloud service providers have started providing these services since last few years, including Microsoft SkyDrive[14], Amazon S3[15], Dropbox[16], Apple iCloud, and Google Drive[8]. In the cloud, there are following two important characteristics that impose challenges to the development of data protection techniques:

- A cloud service can be provided through a chain of service providers. This means the primary provider uses the resources of other providers (the identity to these indirect providers may be unknown to the user). This makes the outsourced files more venerable to attacks and data mining.
- Some possible changes to the indirect providers involved in a cloud service need to be considered also. For example: a participating provider may need to transfer its operations together with users' data to someone else because of the sale of company, a merger, seizure by the government, etc. This means the user's files may remain on several inactive hard drives even after user's request for deletion or close of account.

3. Case Study: Amazon Web Services

Now we will explore the security measures adopted by the largest cloud service provider. Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability, offering the flexibility to enable customers to build a wide range of applications. Helping to protect the confidentiality, integrity, and availability of customers' systems and data is of the utmost importance to AWS, as is maintaining customer trust and confidence.

AWS is a comprehensive cloud services platform that offers compute power, storage, content delivery, and other functionality that organizations can use to deploy applications and services cost-effectivelywith flexibility, scalability, and reliability. AWS self-service means that users can pro-actively address their internal plans and react to external demands when needed[17].

3.1. General Security Measures

AWS incorporate security into its services in accordance with security best practices, and documents how to use the security features. It is important that customer leverage AWS security features and best practices to design an appropriately secure application environment. Ensuring the confidentiality, integrity, and availability of user's data is of the utmost importance to AWS, as is maintaining their trust and confidence[18]. AWS takes the following approaches to secure the cloud infrastructure:

Certifications and accreditations. AWS has in the past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1) report, published under both the SSAE 16 and the ISAE 3402 professional standards. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP).

Physical security. Amazon has many years of experience designing, constructing, and operating large-scale data centers. The AWS infrastructure is located in Amazon-controlled data centers throughout the world. Knowledge of the location of the data centers is limited to those within Amazon who have a legitimate business reasons for this information. The data centers are physically secured in a variety of ways to prevent unauthorized access.

Secure services. Each service in the AWS cloud is architected to be secure. The services contain a number of capabilities that restrict unauthorized access or usage without sacrificing the flexibility that customers demand.

Data privacy. User can encrypt personal and business data in the AWS cloud, and publish backup and redundancy procedures for services so that their customers can protect their data and keep their applications running.

3.2. AWS Infrastructure Security

The process of moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS. This shared model can reduce operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, user assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS provided security group firewall. It is possible for users to enhance security and/or meet more stringent compliance requirements by leveraging technology such as hostbased firewalls, host based intrusion detection/prevention, and encryption [19].

3.3. Security Best Practices

In a multi-tenant environment, everyone is concerned about security. Security should be implemented in every layer of the cloud application architecture. Physical security is off course handled by the service provider, which is an additional benefit of using the cloud. Network and application-level security is user's responsibility. In this section, some specific tools, features and guidelines on how to secure cloud application in the AWS environment is discussed. It is recommended to take advantage of these tools and features mentioned to implement basic security and then implement additional security best practices using standard methods as appropriate.

3.3.1. Protect data in transit

If the data is sensitive or confidential then configure SSL on the server instance. A certificate is requird from an external certification authority like VeriSign or Entrust. The public key included in the certificate authenticates the server to the browser and serves as the basis for creating the shared session key used to encrypt the data in both directions.

3.3.2. Protect stored data

If users are concerned about storing sensitive and confidential data in the cloud, they should encrypt the data (individual files) before uploading it to the cloud. For example, encrypt the data using any open source or commercial PGP-based tools before storing it as Amazon S3 objects and decrypt it after download. This is often a good practice when building HIPAA-Compliant applications [20] that need to store Protected Health Information (PHI). On Amazon EC2, file encryption depends on the operating system. No matter which operating system or technology user choose, encrypting data at rest presents a challenge. If the keys are lost, then the user will lose the data forever and if keys become compromised, the data may be at risk. Therefore, be sure to study the key management capabilities of any products offered and minimize the risk of losing keys.

3.3.3. Protect AWS credentials

AWS supplies two types of security credentials: AWS access keys and X.509 certificates. The AWS access key has two parts: access key ID and secret access key. When using the REST or Query API, user have to use his/her secret access key to calculate a signature to include in the request for authentication. To prevent in-flight tampering, all requests should be sent over HTTPS.

3.3.4. Manage multiple users with IAM

AWS Identity and Access Management (IAM) enables user to create multiple Users and manage the permissions for each of these Users within their AWS Account. A User is an identity (within AWS Account) with unique security credentials that can be used to access AWS Services. IAM eliminates the need to share passwords or access keys, and makes it easy to enable or disable a Users access as appropriate. IAM enables users to implement security best practices, such as least privilege, by granting unique credentials to every User within their AWS account and only grant permission to access the AWS Services and resources required for the Users to perform their job.

3.3.5. Secure Applications

Every Amazon EC2 instance is protected by one or more security groups, named sets of rules that specify which ingress network traffic should be delivered to the instance. User can specify TCP and UDP ports, ICMP types and codes, and source addresses. Security groups provide basic firewall-like protection for running instances. Over time, errors in software are discovered and require patches to fix. All the standard security practices of the pre-cloud era like adopting good coding practices, isolating sensitive data are still applicable and should be implemented.

Conclusion

The revolution of cloud computing has provided opportunities for research in all aspects of cloud computing. We presented the five essential characteristics of cloud computing, three cloud service models, and four cloud deployment models. Research in the secure cloud storage is compounded by the fact that users data may be kept at several locations for either redundancy/ fault tolerance or because the service is provided through a chain of service providers. We explored the security measures adopted by the largest cloud service provider (Amazon web services or AWS) including their infrastructure security and security best practices followed by AWS.

Acknowledgment

We would like to acknowledge the support provided by the department of Information and Computer Science and Deanship of Scientific Research at King Fahd University of Petroleum and Minerals (KFUPM).

References

1. Foster, I., Zhao, Y., Raicu, I., Lu, S.. Cloud computing and grid computing 360-degree compared. In: *Grid Computing Environments Workshop, 2008. GCE '08*. 2008, p. 1–10. doi:10.1109/GCE.2008.4738445.
2. Iankoulova, I., Daneva, M.. Cloud computing security requirements: A systematic review. In: *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on*. 2012, p. 1–7. doi:10.1109/RCIS.2012.6240421.
3. Popovic, K., Hocenski, Z.. Cloud computing security issues and challenges. In: *MIPRO, 2010 Proceedings of the 33rd International Convention*. 2010, p. 344–349.
4. Zhang, Q., Cheng, L., Boutaba, R.. Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications* 2010;**1**(1):7–18. URL: `http://dx.doi.org/10.1007/s13174-010-0007-6`. doi:10.1007/s13174-010-0007-6.
5. Us national institute of standards and technology. `http://csrc.nist.gov/`; 2013.
6. Takabi, H., Joshi, J., Ahn, G.J.. Security and privacy challenges in cloud computing environments. *Security Privacy, IEEE* 2010;**8**(6):24–31. doi:10.1109/MSP.2010.186.
7. Cloud security alliance, security guidance for critical areas of focus in cloud computing v3.0. `https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf`; 2011.
8. Li, M., Yu, S., Ren, K., Lou, W., Hou, Y.. Toward privacy-assured and searchable cloud data storage services. *Network, IEEE* 2013; **27**(4):56–62. doi:10.1109/MNET.2013.6574666.
9. Google drive owns everything you upload? privacy policy concerns remain. `http://nvonews.com/2012/04/26/google-drive-owns-everything-you-upload-privacy-policy-concerns-remain/`; April 26, 2012.
10. Edwards, C., Riley, M.. Sony data breach exposes users to years of identity-theft risk. `http://www.bloomberg.com/news/2011-05-03/sony-breach-exposes-users-to-identity-theft-as-credit-card-threat-recedes.html`; 2011-05-03.
11. Yin, S. Dropbox accounts were accessible by anyone for four hours. `http://www.pcmag.com/article2/0,2817,2387343,00.asp`; June 21, 2011.
12. Takabi, H., Joshi, J., Ahn, G.J.. Securecloud: Towards a comprehensive security framework for cloud computing environments. In: *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual*. 2010, p. 393–398. doi:10.1109/COMPSACW.2010.74.
13. Naresh Kumar, M., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A., Kumar, M.. Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. In: *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on*. 2012, p. 535–539. doi:10.1109/CICN.2012.149.
14. Microsoft azure. `http://www.windowsazure.com/`; 2013.
15. Amazon s3. `http://aws.amazon.com/s3`; 2013.
16. Dropbox - your stuff, anywhere. `https://www.dropbox.com/`; 2013.
17. Varia, J., Mathew, S.. Overview of amazon web services. `http://aws.amazon.com/whitepapers`; March 2013.
18. Amazon web services: Overview of security processes. `http://aws.amazon.com/security/`; June 2013.
19. Bragg, R.. The encrypting file system. `http://technet.microsoft.com/en-us/library/cc700811.aspx`; 2009.
20. Amazon web services team, creating hipaa-compliant medical data applications with aws. `http://media.amazonwebservices.com/AWS_HIPAA_Whitepaper_Final.pdf`; 2009 – 04 – 01.